# Formal Methods for Railway Systems: a Survey of Research and Technology Transfer Projects

Davide Basile[1], Maurice H. ter Beek[1], Giovanna Broccia[1], Stefania Gnesi[1], Franco Mazzanti[1], Giorgio Oronzo Spagnolo[1], Stefano Bacherini[3], Carlo Becheri[3], Daniele Grasso[4], Gianluca Magnani[3], Matteo Tempestini[3], Niccolò Zingoni[3], and Alessio Ferrari(✉)[2,1]

[1] Formal Methods and Tools lab, CNR–ISTI, Pisa, Italy
{davide.basile,maurice.terbeek,giovanna.broccia,
stefania.gnesi,franco.mazzanti,spagnolo}@isti.cnr.it
[2] University College Dublin, School of Computer Science, Dublin, Ireland
alessio.ferrari@ucd.ie
[3] Alstom Ferroviaria S.p.A., Firenze, Italy
{stefano.bacherini,carlo.becheri,gianluca.magnani,
matteo.tempestini, niccolo.zingoni}@alstomgroup.com
[4] Digitense S.r.l., Firenze, Italy
danielegrasso@digitense.it

**Abstract.** This paper offers a retrospective on collaborative projects that involved Alessandro Fantechi and the authors over the past two decades, from the shared perspective of the Formal Methods and Tools (FMT) lab of the Italian National Research Council (CNR) and former collaborators at General Electric (GE) Transportation and Alstom. The focus is on research and technology transfer efforts in the field of formal methods for railway systems, where Alessandro Fantechi's contributions have been central to the development and application of formal specification, model-based verification, and tool-supported analysis. Joint work in projects such as ASTRail, 4SECURail, and TRACE-IT, as well as in industrial collaborations with Alstom and GE Transportation Systems illustrates the sustained impact of these activities on both academic research and industrial practice. This contribution reflects on the evolution of these efforts, the formal methods adopted, and the outcomes achieved in terms of methodologies, tools, and integration into safety-critical development processes. It also highlights the collaborative environment fostered across institutions and organizations, which has been instrumental in advancing the use of formal methods in the railway domain.

**Keywords:** Formal Methods · Railways · Model-based Development

## 1 Introduction

Alessandro Fantechi is well recognized as one of the foremost experts on the application of formal methods (FMs) and tools to railway systems [51,53,52,55,31].

He is the most cited researcher in Scopus when searching for publications on "formal method" and "railway". He is member of the steering committee of the dedicated conference series RSSRail on *Reliability, Safety, and Security of Railway Systems: Modelling, Analysis, Verification, and Certification.*

Alessandro is an authority in the field of FMs [40] and member of the board of the ERCIM Working Group on Formal Methods for Industrial Critical Systems (FMICS), which organises a dedicated annual conference for three decades now.[5]

Alessandro's involvement in the railway industry is also witnessed by the numerous collaborations he has had with the main companies in this sector, such as Ansaldo Ferroviaria, Alstom Ferroviaria, General Electric (GE) Transportation Systems, SIRTI s.p.a., and others. Alessandro Fantechi is also a member of the Strategic Technological Steering Committee (STSC) of DITECFER S.c.ar.l (an acronym for "District for Railway Technologies, High Speed, Network, Safety & Security"), whose objective is to promote collaboration, innovation, research and development among its members to make them more competitive and support integrated internationalization in foreign markets.

Arguably the first applications of FMs and tools to railway designs in which Alessandro was involved concern two exemplary cases. In both cases, a CCS dialect is used to model the example, ACTL—an action-based extension of CTL [48,49]—is used to specify the logical properties to be verified, and EMC—the first model checker developed by E.M. Clarke et al. [43,44]—is used to perform the formal verification. In [46], a road crossing a railway is modeled and both safety ("it never happens that both a car and a train are able to cross") and liveness ("whenever a train (a car) approaches, it eventually crosses") properties are model checked. In [47], a circular railway, divided into six track sections, with two trains is modeled and the property "it never happens that both trains are running on the same track section" is model checked.

In the context of industrial collaborations, which have characterized Alessandro's career, one of his first experiences of applying FMs and tools to railway systems concerns the formal verification of a computer-based interlocking system provided by the Italian railway company Ansaldo Trasporti. The system was modeled in CCS and a number of safety properties expressed in ACTL were verified using the ACTL model checker AMC developed at CNR [6,36]. This experience was followed a few years later by related experiences on the specification and validation of fault-tolerance mechanisms for safety-critical systems, among which a railway interlocking system, inside the EU project GUARDS [35], and by a number of other national and international projects dedicated to the railway domain, discussed in more detail in the remainder of this paper.

**Outline** In Section 2, we discuss some of Alessandro Fantechi's aforementioned collaborations with the Railway industry. In Section 3, we describe the regional project TRACE-IT. In Sections 4 and 5, we describe the EU H2020 projects ASTRail and 4SECURail, financed under the Shift2Rail initative. In Section 6, we describe the regional project STINGRAY. In Section 7, we describe the

[5] https://fmics.inria.fr/

NextGenerationEU project MOST (National Center for Sustainable Mobility), Spoke 4: Rail Transportation, financed under the Italian National Recovery and Resilience Plan (PNRR). Section 8 provides a summary of contributions and lessons learned, while Section 9 concludes the paper.

## 2 GE and Alstom Collaborations

Alessandro Fantechi has collaborated extensively with railway signaling manufacturers, including General Electric (GE) Transportation Systems and Alstom Ferroviaria (now part of Alstom), on projects involving FMs, model-based development, and requirements analysis in safety-critical railway systems. These collaborations span interlocking systems, automatic train protection (ATP) systems, and the detection of defects in requirements documents. The projects emphasize the adoption of formal modeling and verification techniques, such as SDL (Specification and Description Language), Statecharts, model-based testing, abstract interpretation, and natural language processing (NLP) for requirements quality assurance.

Early work with industry explored modeling choices for complex interlockings, contrasting "geographical" vs. "functional" Statechart decomposition and its impact on understandability and reuse [10]. In parallel, a component-oriented SDL specification—explicitly based on an interlocking model from GE—was validated using MSC-driven techniques and coverage criteria [9]. A companion experience report describes the overall adoption path of FMs in a signaling manufacturer, detailing drivers like European standards and process constraints [8]. Foundational background on distributed interlocking modeling and the role of FMs is reported in [11]. A broader experience report in [8] detailed the adoption of FMs at GE, including SDL-based modeling of interlocking systems. External factors like European regulations (e.g., EN 50128) and university collaborations drove the choice of notations and tools, leading to internal acceptance.

A later collaboration with GE's Safety & Validation group engineered a *model-extraction* pipeline from delivered interlocking logic: the extracted model is (1) executed against planned test suites to accelerate fault finding and reduce target testing cost, and (2) formally verified with an iterative process combining slicing and CEGAR-like refinement to tame complexity [38]. A short, practice-oriented precursor shows how exercising the extracted model enables order-of-magnitude faster feedback than on-target tests [37].

The Metrô Rio ATP case study in [61] applied Simulink/Stateflow for on-board equipment development. A two-phase verification approach (model-based testing and abstract interpretation) ensured functional correctness and runtime error freedom, with formal verification as a side activity. Results showed reduced bugs and verification costs. Reference [62] reported restructuring unit-level verification at GE from code-based to model-based testing plus abstract interpretation, achieving 70% cost reduction and improved bug detection on two case studies. Complementing this, a set of guidelines codified modeling rules aimed at *qualified code generation* in the railway domain, explicitly contextualized at

GE and their ATP products [57]. In [58], lessons from adopting formal model-based design at GE were reviewed. Challenges included defining a safe subset of Simulink/Stateflow, ensuring code-model conformance via back-to-back testing, and integrating with EN 50128 processes. Incremental refinements across projects enhanced safety and cost-effectiveness. A final magazine publication summarizing all these experiences was published in IEEE Software [59].

Recent work addressed requirements quality in the railway domain using NLP techniques. With Rosadini et al. [72] and Ferrari et al. [60], Fantechi applied NLP patterns with the GATE tool to detect defects in 1866 requirements from a railway signaling manufacturer (likely GE/Alstom context). Patterns identified vagueness, optionality, and other issues, complemented by the SREE tool for ambiguity detection. The study highlighted discrepancies between manual and NLP-based analysis, suggesting hybrid approaches for industrial use. Although not strictly FM studies, these works focus on preparatory activities in requirements, which are needed for later translation into formal logic expression, an area that is seeing an increasing interest thanks to recent developments in Large Language Models (LLMs) [66].

Across two decades, these collaborations demonstrate how FMs and model-based techniques were concretely *embedded in industrial practice*:

- For **interlockings**, the pathway led from exploratory modeling choices and SDL validation with GE artefacts [10,9] to *scalable validation processes* that extract models from logic and leverage testing and model checking [37,38].
- For **ATPs**, the emphasis was on *process integration*: safe modeling subsets, evidence of model–code conformance, and certification-friendly workflows [58,57], supported by a published product case [61].
- For **requirements**, the Alstom collaboration shows the feasibility and limits of NLP-based defect detection at scale, and how results feed back into both tools and company practices [60].

## 3 TRACE-IT

TRACE-IT (Train Control Enhancement via Information Technology) was a 4-year project started in 2011, funded by the Tuscany Region. It was coordinated by ECM (now Caterpillar) with the participation of CNR and the University of Florence. The project's objective was the development of an ATP system and an Automatic Train Control (ATC) system based on ERTMS/ETCS levels 2 and 3, and an innovative Communication Based Train Control System (CBTC).

The involvement of CNR–ISTI in the project centered around the development of a demonstrator of the ATC system integrating the ECM components with a custom Automatic Train Supervision (ARS) system based on a specific railway layout selected as case study (cf. Fig. 1).

The case study used for the demonstrator was supposed to model a CBTC-based metro system, in which 8 trains have the mission to safely and continuously loop in the system. The developed ATS system was not concerned with modeling specific timetables at the various stations, but focused on the more challenging

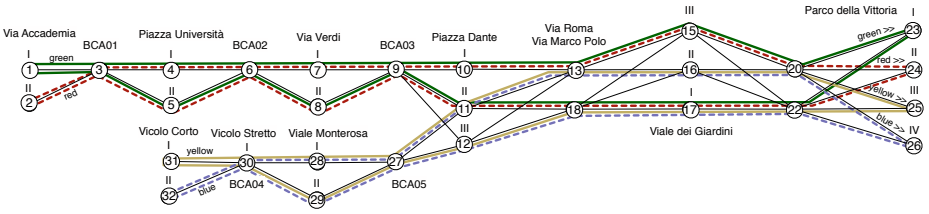


**Fig. 1.** The railway layout user for the case study (from [71])

problem of defining a strategy for avoiding deadlocks in the system and on formally proving its correctness [70]. The formal proof was achieved by modeling the layout and the strategy with the UMC tool, and using the UMC on-the-fly model-checking features to prove the absence of (partial) deadlocks (i.e., it never happens that a train is no longer able to continue its mission).

The strict collaboration between academia and the industrial partner has been very productive for increasing the awareness of CNR–ISTI concerning railway-related topics, and for increasing the awareness of the industrial partner towards advanced methods of system modeling, analysis and verification.

From the point of view of CNR–ISTI, the selected case study has been the starting point for further studies on formal methods diversity. After the project, in fact, at CNR–ISTI, we performed the experiment of modeling and verifying the same TRACE-IT case study using nine other different formal methods approaches [69,68] (SPIN, NuSMV, mCRL2, CPN, FDR4, CADP, TLA+, ProB, and UPPAAL). This complex experiment has been useful for better understanding the position of our UMC tool in the context of the state of the art of formal modeling and verification, and for gaining valuable knowledge of the advantages and difficulties of the various frameworks. This acquired knowledge proved to be very useful in enriching the CNR's participation in other projects.

The TRACE-IT project also produced other outputs focused on CBTC. Specifically, in [65], a global model for CBTC systems was developed by combining semi-formal modeling with product line engineering, based on a comprehensive market analysis. The methodology enabled the derivation of novel CBTC products and system requirements for individual components. Scenario-based requirements elicitation, supported by rapid prototyping, was employed, with requirements written in constrained natural language (CNL) and evaluated using NLP techniques to enhance quality. The approach aimed toward formal requirements representation and was applied to derive a novel CBTC architecture and a prototype tool showcased in collaboration with ECM, the company involved in the project, demonstrating practical implementation.

## 4 ASTRail

ASTRail (SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block validation) [74] was a 2-year project

funded by the European Union under the Shift2Rail initiative, started in 2017 and coordinated by ISMB, with the participation of SIRTI S.p.A., Ardanuy Ingenieria, ENAC, UNIFE, and CNR–ISTI. The involvement of CNR–ISTI centered on review and assessment of the main formal modeling and verification languages and tools used in the railway domain, with the aim of evaluating the actual applicability of the most promising ones to a moving block signaling system model provided by an industrial partner. This has been achieved in four steps:

1. A survey on the state of art on the use of FMs in Railways;
2. Experimentations of an extensive set of FM tools and systematic evaluation;
3. A trial application of a moving block system with a short list of tools;
4. A final validation of the designs of the moving block and the ATO system.

The first two steps involved a detailed study of the state-of-the-art, by scrutinizing the existing literature, performing surveys, observing recents projects, and carrying out a set of experimentations with a list of 14 candidate methods and tools to get first-hand experience concerning their usability, availability and efficacy (cf. Fig. 2). These studies have been published in [7,63,56,28,7,64].

The last two steps have been performed by developing and modeling the system requirements starting from descriptions in the form of UML statecharts. A short list of frameworks (Simulink, UMC, and ProB) has been used to get a feeling of three different kinds of approaches: fully industrial (Simulink), experimental academic (UMC), and mature academic (ProB). The moving block system was also formalized and analyzed using UPPAAL and the original Simulink design, and the results have been published in [12,15,16].

The result of the survey and classification of the state-of-the-art in the application of FMs in the railway sector has been very successful and has been cited and referred to by many studies on the use of FMs.

The first-hand modeling with the final three selected frameworks has allowed us to experience directly the actual importance of standard (framework-independent) notations like UML, and the importance of simulation and animation, at different levels of abstraction, to achieve a deep understanding of the system behavior. The formal verification of the systems has proved useful to get a more complete picture of the system under development, but at a much higher cost and requiring particularly well-trained personnel.

As the modeled systems are just academic case studies and not parts of any real industrial product, the impact of the formal experimentation on the actual software development process of the industrial partner has not gone beyond an increased awareness of the potentialities of FMs.

## 5 4SECURail

4SECURail (Formal methods and CSIRT for the railway sector) [73,4] was a 2-year project funded by the European Union under the Shift2Rail initiative, started in 2019 and coordinated by Ardanuy Ingegneria S.A. The project had two completely independent objectives, involving different and non-interacting

| Category | Name | SPIN | Simulink | nuXmv | ProB | AtelierB | UPPAAL | SCADE | FDR4 | CPN Tools | CADP | mCRL2 | SAL | TLA+ | UMC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Development Functionalities | Specification/ Modeling | TEXT | GRA | TEXTIN | TEXT | TEXT | GRA | GRA | TEXTIN | GRA | TEXTIN | TEXT | TEXTIN | TEXT | TEXT |
| | Code Generation | NO | YES | NO | NO | YES | NO | YES | NO | NO | YES | NO | NO | NO | NO |
| | Document / Report Generation | PARTIAL | YES | NO | PARTIAL | PARTIAL | PARTIAL | YES | PARTIAL | PARTIAL | PARTIAL | PARTIAL | NO | NO | PARTIAL |
| | Requirements Traceability | NO | YES | NO | NO | NO | NO | YES | NO | NO | NO | NO | NO | NO | NO |
| | Model refinement | NO | YES | NO | YES | YES | NO | YES | YES | NO | NO | NO | NO | NO | NO |
| Verification Functionalities | Simulation | TEX | GRA | TEX | MIX | NO | GRA | GRA | TEX | GRA | TEX | TEX | TEX | NO | TEX |
| | Supported problem size | LARGE | LIMITED | LARGE | MEDIUM | MEDIUM | MEDIUM | LIMITED | LARGE | LIMITED | LARGE | MEDIUM | LARGE | MEDIUM | MEDIUM |
| | Formal Verification | MC-L | MC-I | MC-L,MC-B | MC-L,MC-B, TP, RF | TP, RF | MC-L | MC-I | RF | MC-B | MC-B | MC-B | MC-L, TP | MC-L, TP | MC-B |
| | Model-based Testing | NO | YES | NO | YES | NO | NO | YES | NO | NO | YES | NO | YES | NO | NO |
| | Time related properties | NO | YES | YES | NO | NO | YES | YES | YES | YES | NO | YES | YES | NO | NO |
| | Probability properties | NO | NO | NO | NO | NO | YES | NO | NO | NO | NO | NO | NO | NO | NO |
| Language Expressivenes | Nondeterminism | INT | EXT | INT,EXT | INT,EXT | INT,EXT | INT | EXT | INT,EXT | INT | INT,EXT | INT,EXT | INT,EXT ASYNCH, | INT | INT ASYNCH, |
| | Concurrency | ASYNCH | NO | SYNCH | NO | NO | SYNCH | SYNCH | ASYNCH | ASYNCH | ASYNCH | ASYNCH | SYNCH | ASYNCH | SYNCH |
| | Temporal Aspects | NO | YES | NO | NO | NO | YES | YES | YES | YES | NO | NO | YES | NO | NO |
| | Probability | NO | NO | NO | NO | NO | YES | NO | NO | NO | NO | NO | NO | NO | NO |
| | Language Modularity | HIGH | HIGH | MEDIUM | LOW | LOW | MEDIUM | HIGH | HIGH | HIGH | HIGH | LOW | MEDIUM | MEDIUM | HIGH |
| | Supported Data Structures | BASIC | COMPLEX | BASIC | COMPLEX | COMPLEX | COMPLEX | COMPLEX | COMPLEX | COMPLEX | COMPLEX | COMPLEX | COMPLEX | COMPLEX | COMPLEX |
| Tool Flexibility | Backward Compatibility | LIKELY | LIKELY | LIKELY | LIKELY | MODERATE | LIKELY | LIKELY | MODERATE | LIKELY | LIKELY | LIKELY | MODERATE | MODERATE | MODERATE |
| | Standard Input Format | YES | PARTIAL | YES | YES | YES | PARTIAL | PARTIAL | YES | PARTIAL | YES | YES | YES | YES | YES |
| | Import/Export | MEDIUM | LOW | MEDIUM | HIGH | MEDIUM | LOW | LOW | MEDIUM | MEDIUM | HIGH | HIGH | MEDIUM | LOW | LOW |
| | Modularity of the Tool | LOW | HIGH | LOW | LOW | MEDIUM | LOW | HIGH | LOW | LOW | LOW | LOW | LOW | LOW | LOW |
| | Team Support | NO | NO | NO | NO | YES | NO | NO | NO | NO | NO | NO | NO | NO | NO |
| Maturity | Industrial Diffusion | MEDIUM | HIGH | MEDIUM | RAILWAY | RAILWAY | MEDIUM | RAILWAY | LOW | MEDIUM | MEDIUM | LOW | LOW | MEDIUM | NO |
| | Stage of Development | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES | NO |
| Usability | Customer Support | PARTIAL | YES | PARTIAL | YES | YES | YES | YES | PARTIAL | PARTIAL | PARTIAL | PARTIAL | PARTIAL | PARTIAL | PARTIAL |
| | Graphical User Interface | LIMITED | YES | NO | PARTIAL | PARTIAL | PARTIAL | YES | LIMITED | PARTIAL | LIMITED | LIMITED | NO | LIMITED | PARTIAL |
| | Easy to Use | MEDIUM | BASIC | MEDIUM | MEDIUM | ADVANCED | MEDIUM | BASIC | MEDIUM | MEDIUM | ADVANCED | ADVANCED | ADVANCED | ADVANCED | MEDIUM |
| | Quality of Documentation | GOOD | EXCELLENT | GOOD | GOOD | EXCELLENT | GOOD | EXCELLENT | EXCELLENT | GOOD | GOOD | GOOD | GOOD | GOOD | LIMITED |
| Company Constraints | Cost | FREE | PAY | MIX | FREE | FREE | MIX | PAY | MIX | FREE | MIX | FREE | FREE | FREE | FREE |
| | Supported Platforms | Windows, Linux, macOS | Windows, Linux, macOS | Windows, Linux, macOS | Windows, Linux, macOS | Windows, Linux, macOS | Windows, Linux, macOS | Windows | Windows, Linux, macOS | Windows | Windows, Linux, macOS | Windows, Linux, macOS | Windows, Linux, macOS | Windows, Linux, macOS | Windows, Linux, macOS |
| | Complexity of License Management | EASY | ADEQUATE | EASY | EASY | EASY | MODERATE | ADEQUATE | MODERATE | EASY | MODERATE | EASY | EASY | EASY | EASY |
| | Easy to Install | YES | YES | YES | YES | YES | YES | YES | YES | YES | PARTIAL | YES | YES | YES | YES |
| [illegible] specific Criteria | CENELEC Certification | NO | PARTIAL | NO | NO | NO | NO | YES | NO | NO | NO | NO | NO | NO | NO |
| | Integration into the CENELEC Process | MEDIUM | YES | MEDIUM | YES | YES | MEDIUM | YES | MEDIUM | MEDIUM | MEDIUM | LOW | LOW | LOW | LOW |
| | | SPIN | Simulink | nuXmv | ProB | AtelierB | UPPAAL | SCADE | FDR4 | CPN Tools | CADP | mCRL2 | SAL | TLA+ | UMC |

**Fig. 2.** The ASTRail tool evaluation table (from [7])

teams. A first activity, led by Hit Rail B.V. with the collaboration of UIC and Tree Technology, was targeted at the design and delivery of a prototype of "Computer Security Incident Response Team" (CSIRT). A second activity, led by CNR–ISTI with the collaboration of SIRTI (later MerMec STE) and Fit Consulting, had as objective the setup of a FMs Demonstrator for the evaluation, in terms of costs, benefits and required learning curve, of the impact of the use of FMs for the rigorous specification of the components of railway signaling infrastructures.

At the European level, the importance of a set of rigorous railway standards like UNISIG, ERTMS, and EULYNX to guide the development of a common european railway infrastructure is well recognized. Railway standards are however written in natural language, often with the support of UML-like statechart images to highlight the main state transition concepts of the protocols, and this leaves spaces to potential ambiguities, incompleteness, and inconsistencies. It is therefore of high interest to evaluate how the introduction of FMs might be of help in the strengthening of the standards, and at what cost.

It is important to observe that the focus of CNR's activity, in which Alessandro Fantechi was involved, was the evaluation of the introduction of FMs from the point of view of the infrastructure managers, interested in the definition of high-quality standards, and only secondarily to the point of view of the system providers, potentially interested in the rigorous development of commercial products conforming to the standards or, more specifically, conforming to some custom developed system requirements specification.

In more detail, the "FMs Demonstrator" activity started with the definition of the tools and methodologies to be used, as described in [1,14]. UML/SysML was selected as the starting point notation for the construction of an operational model of the system under specification. Indeed UML fragments often appear inside the standard documents, and UML has been often used as a starting point for formal analysis [14,67,45,41,50]. For this reason, UML/SYSML may play the role of a bridge between for the formal and industrial world.

The tool UMC[6] was selected for initial fast prototyping of the systems and for their formal analysis. UMC is an open-access, open-source, UML-based model checker developed at CNR–ISTI that had already been used in other railway related projects. The developed UML models were translated also in the formal notations used by ProB and CADP/LNT to achieve a more complete and mature analysis of the systems. A partial effort has also been made on the use of the same UML models as a starting point for an industrial model-based framework (Sparx EA) to experiment a possible point of view from the developer side [2,26,25].

The overall impact of the formal modeling approach confirmed (cf. [2,3]) the actual usefulness of FMs for the identification of inconsistencies, missing points, and ambiguities in initial natural language requirements, has allowed to gain deeper insights on the intended system evolutions, and has allowed the generation or more robust specification documents [33] (cf. Fig. 3).

[6] http://fmt.isti.cnr.it/kandisti/

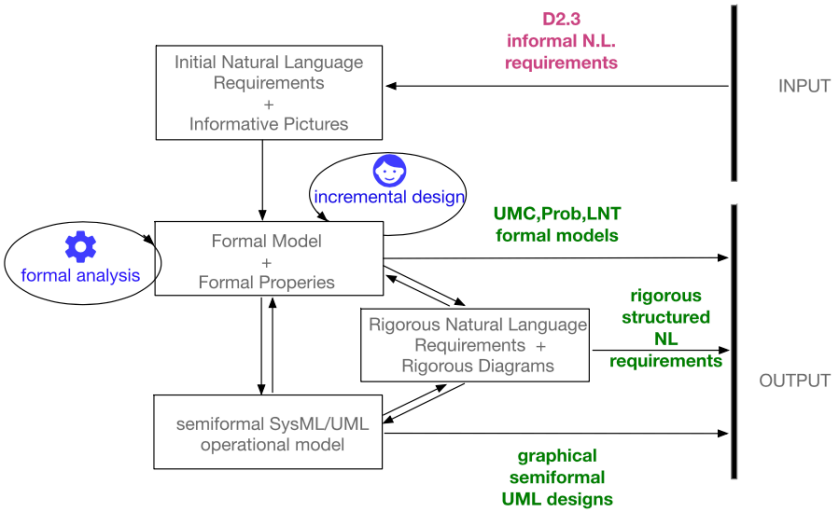


**Fig. 3.** The 4SECURail formal modelling process (from [4])

The cost/benefit analysis [5,32] provided a rare insight on the economic impact of the introduction of FMs in the process of system requirements definition, both in terms of investments (CAPEX) and operational costs (OPEX) and confirmed the economic advantages of the approach.

The formal modeling experiment was conducted on a fragment of the so-called RBC/RBC handover protocols, following a case study selected by SIRTI [3] based on the standards UNISIG SUB-039 and SUB-098, and all the generated UMC, Prob, and LNT models have been made publicly available [67,26].

Another output in which Alessandro Fantechi has been involved, was to use the tool UPPAAL to model and analyze the case study of the 4SECURail project [24]. This work involved an M.Sc. student at the University of Florence, trained in FMs in a postgraduate course at the University of Florence, taught by Alessandro Fantechi. The output of this analysis has been used as input to the cost and benefit analysis phase, as well as uncovering issues in the standards UNISIG SUB-039 and SUB-098, thereby showcasing the efficacy of the application of FMs to a railway industrial project.

From the academic point of view the project was quite successful. Its results were presented in several venues, stimulating the implementation of several ideas for improving the UMC verification framework, and raising many points worthwhile of further studies. Among the points that would need further investigation, it is worth mentioning a reasonably clear and tool-supported formal semantics for simple UML/SYSML designs, the relation between abstract requirements, system requirements, and operational models, the possible integration of model-driven frameworks with formal verification frameworks, and the construction of bridges among different verification frameworks to enable the exploitation of their diversity to achieve a more complete and user friendly analysis of a system.

## 6 STINGRAY

STINGRAY (SmarT station INtelliGent RAilwaY was a 2-year project, started in 2018, funded by the Tuscany Region. It was coordinated by ECM with the participation of CNR and the University of Florence. STINGRAY addressed the role of the railway station, traditionally seen as a meeting point for a city, to enhance its importance and integration into the smart city of the future.

Although railway stations are a central hub of the city, a primary point of aggregation in the urban environment, they traditionally have a private energy distribution and communication system. The main reasons for this are to ensure uninterrupted power supply and security, but this isolation has two main drawbacks. First, it prohibits integration with "smart cities", in which, ideally, information between different transport systems (i.e., bike sharing, car sharing, urban transport) is synergically exploited. Second, the station system fails to benefit from modern energy-saving techniques.

To this aim, the design and development of a station communication infrastructure was studied, integrating powerline and wireless technologies (cf. Fig. 4). Powerlines are utilized to enable a more efficient management of machinery and energetic resources. The concrete goals of the project were:

1. To realise a LAN over the station plants using power line and wireless technologies;
2. To allow control and monitoring of station equipment via Supervisory Control And Data Acquisition (SCADA), in particular railroad switch heaters;
3. To create value-added services for both customers and railway staff, such as connectivity, monitoring fault prediction service (FPS), video surveillance, environmental surveying and integration and access to so-called smart city infomobility services, in particular the energy management service (EMS);
4. To optimize existing strategies for managing energy consumption within the station, to avoid wasting energy.

The case studies of STINGRAY provided by the industrial partners from the railway domain concerned station lighting and the heating of the railroad switches in ice conditions.

Railroad switch heaters assure correct working of switches in case of ice and snow through a central control unit in charge of managing policies of energy consumption while satisfying reliability constraints. Although apparently a rather focused system, with restricted functionalities, it represents very well the peculiarities of a cyber-physical system: physical components (the heater), cyber components (the heating policies and the related coordinator), stochastic aspects (failure events and weather forecasts), and logical/physical dependencies. The adopted policy of energy consumption was an on/off strategy based on temperature thresholds (both for turning off and on the energy).

In [13], Fantechi et al. addressed the railroad switch heaters case study. It was modeled and analyzed with stochastic activity networks (SAN) and Möbius on the one hand and with stochastic hybrid automata (SHA) and UPPAAL SMC on the other hand, followed by a comparison of the two methodologies.

The system was initially modeled and analyzed in [18,17,19,23] using Möbius and SAN. It was assumed that heaters have different priorities in accessing the energy resources, and the energy consumption policy was tuned to adapt both to the different priorities of the heaters and to the different periods of the day. The model was equipped with a logical part, representing the energy consumption policy, and a physical part, modeling temperature behavior and weather.

In [22], the same system was modeled and analyzed with UPPAAL SMC and SHA. Temporal logic was used instead of Markov reward models to capture the measures of interest, namely energy consumption and probability of failure. The logic of the energy policy was verified in [21] against the progress of interactions, to prevent deadlocks in communications between the different components.

The two formalizations were compared in [23] to highlight the pros and cons of each approach. Lastly, in [20], the methodology was generalized to automatically map an automata-based model, representing a qualitatively verified energy consumption policy, to a stochastic Petri net dialect. This enabled the inclusion of stochastic behavior (e.g., weather conditions) for quantitative evaluation.

At the end of the project, the design of future smart station lighting management applications was addressed, with the aim of reducing station illumination whenever (time) and wherever (space) possible while guaranteeing minimum illumination levels as required by legislation. A station platform's (ceiling) lights (LEDs) are equipped with a data acquisition module called MADILL. A C-MAD unit collects the messages from each MADILL and it is equipped with brightness sensors and commands to switch (groups of) lights on, off, or dim them.

In [30], the authors considered user-experience related requirements such as "*passengers should always be able to rely on an illuminated pathway when getting on or off a train, from the main entrance, to the platform*", to avoid passengers transiting or waiting in non-illuminated areas, with the associated risks (e.g., theft or injury), or "*there should be an illumination level greater than $x$ on platforms where a train is about to arrive, even if the train is late*". Such requirements are inherently spatial or spatio-temporal, as they deal with the possibly complex reachability relations and pathways of a train station.

The authors described how to tackle these requirements in an experiment aimed at identifying poorly illuminated platform areas of the Pistoia railway station by the application of spatial model-checking techniques and the VoxLogicA model-checking tool [34]. Provided with concrete images and given a threshold on the illumination value, VoxLogicA managed to compute both areas that are and parts of the platforms that are not sufficiently illuminated.

The application of formal methods and tools to the STINGRAY case studies described above contributed successfully to the project's third and fourth goals.

## 7 MOST Spoke 4

Spoke 4 "Rail Transportation" of the Sustainable Mobility National Research Center (MOST) concerns a project, started in 2022, which received funding from the European Union NextGenerationEU framework through the Italian National Recovery and Resilience Plan (PNRR).

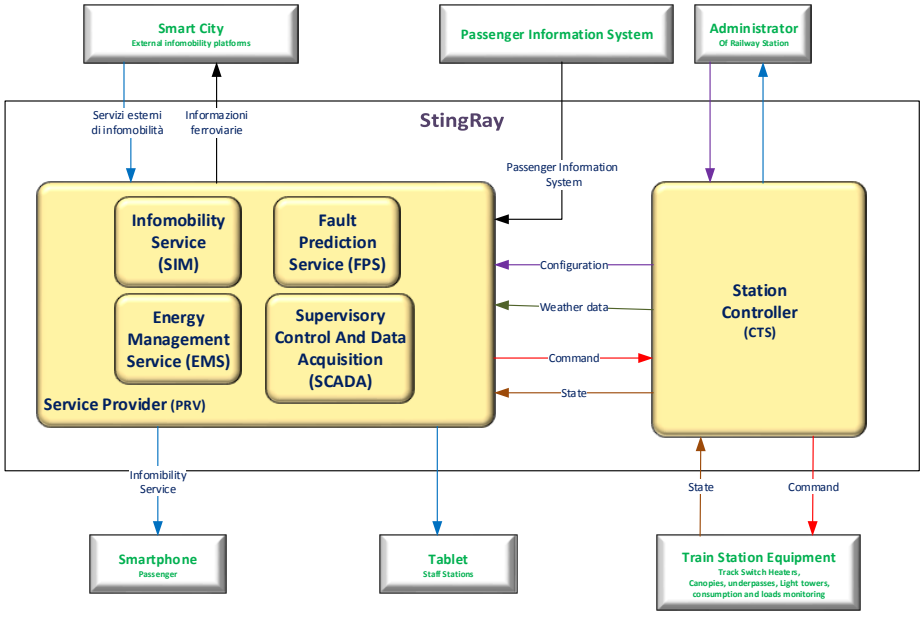


**Fig. 4.** The STINGRAY architecture

The initiative aims to promote sustainable and digital innovation in mobility and transportation systems through strategic collaborations between academia and industry, and Spoke 4 focuses on the development of advanced methodologies and tools for enhancing the efficiency, safety, and resilience of railway systems.

In Spoke 4, CNR–ISTI coordinates WP3 (Digitization of railway transport) and task T3.1 (Learning formal models for predictive maintenance), and participates in task T1.3 (Resilient and sustainable railway infrastructure) of WP1 (Increase of capacity of railway transport) coordinated by Alessandro Fantechi.

In this section, we focus on the participation in task T3.1, in which CNR–ISTI actively explored predictive maintenance strategies through the integration of formal methods, machine-learning techniques, and human-centred design practices. The activities were carried out in close collaboration with a consortium of academic and industrial partners, including the University of Florence (with Alessandro Fantechi as the referent), the University of Naples Federico II, Trenord, and Lutech. As part of these activities, CNR–ISTI led two parallel yet complementary lines: (1) the development of data-driven approaches for anticipating failures in railway subsystems such as the Traction Control Unit (TCU), and (2) the design of an interactive dashboard that aggregates predictive insights from multiple data-driven approaches and facilitates decision-making for different classes of users (maintenance and engineering personnel).

The development of data-driven approaches for predicting railway maintanance needs progressed from classical statistical forecasting models to super-

vised machine-learning algorithms. In [54], an analysis of time-series forecasting methods applied to diagnostic event logs was conducted. Classical models including but not limited to Autoregressive Integrated Moving Average (ARIMA) and Seasonal ARIMA (SARIMA) were tested on a dataset provided by Trenord. The dataset originates from Trenord's fleet, where an on-board diagnostic platform continuously collects data from each train and transmits it to a wayside system for storage and analysis. The performance of these models was evaluated against a Random Walk baseline, using Root Mean Square Error (RMSE) as the evaluation metric. Results were promising, particularly concerning ARIMA and SARIMA algorithms. These models provided useful baselines and helped uncover temporal properties of the data, but their predictive accuracy proved highly dependent on the characteristics of each train and limited in capturing heterogeneous and non-linear patterns across fleets.

Building on these insights, we explored the adoption of supervised machine-learning methods for predictive maintenance. These methods offer greater flexibility in modeling complex, non-linear, and multivariate relationships in railway diagnostic data. To this end, time-series diagnostic logs were reformulated into a supervised learning problem through a sliding-window approach, where fixed sequences of past observations were used to predict future events. Several families of models were evaluated: tree-based ensembles (Random Forests, Gradient Boosting, and XGBoost), support vector machines, and neural networks (ANNs, LSTMs, and Temporal Convolutional Networks). Among these, XGBoost consistently provided the best trade-off between recall and precision, a crucial balance in predictive maintenance where false negatives (i.e., missed failure predictions) must be minimized for safety reasons. At the same time, limitations were identified, notably the risk of performance degradation when failure patterns evolve or sensor drift introduces non-stationarity, underscoring the need for periodic model retraining and recalibration.

Parallel to algorithmic development, CNR–ISTI employed requirements engineering and user-centred design methodologies to ensure that the predictive maintenance dashboard was aligned with the operational workflows and stakeholder needs of Trenord. The dashboard is meant to be integrated into Trenord's existing maintenance platform and to present the outcomes of different predictive approaches developed within the project: machine-learning algorithms implemented by Lutech, fault-tree analysis developed at the University of Florence by Alessandro Fantechi et al. [42], and clustering and filtering techniques contributed by the University of Naples. The platform supports both fleet-level and train-specific views, allowing maintenance personnel to access detailed information on individual predictions, while engineering personnel is provided with dedicated pages offering in-depth analyses across all three methodologies.

The development of the dashboard followed an iterative, user-centred process articulated in four phases: requirements elicitation, prototyping, interactive mock-ups, and final specification. Through meetings, focus groups, and task observations, CNR–ISTI gathered explicit and implicit knowledge of Trenord's workflows, building a clear picture of user goals and challenges. Early low-fidelity

mock-ups were then used to stimulate discussion and refine requirements, before evolving into interactive prototypes that combined manual design with AI-assisted mock-up generation [39]. These prototypes were reviewed and refined in successive iterations, ensuring alignment with stakeholder expectations. The process culminated in a consolidated requirements document, serving as a shared reference for all partners and providing the foundation for the further implementation and integration of the dashboard into Trenord's diagnostic platform.

## 8 Summary: Achievements and Limitations

This survey has summarized over two decades of studies that were either led by or involved Alessandro Fantechi. Table 1 highlights contributions and references (cf. also [31,27]). The overall trajectory that emerges is one of steady maturation: from early feasibility studies and targeted formal verifications, through the consolidation of methods and tools, to demonstrators and processes that increasingly satisfy the constraints of certification-oriented, safety-critical development. Across projects on interlocking and ATP functions, on standard- and requirement-level modeling, and on station-level innovation, the repeated pattern was to start from industrially understandable notations and artefacts, to formalize incrementally where risk and ambiguity were highest, and to close the loop with empirical evidence about costs and benefits.

### 8.1 Achievements

A central outcome of these efforts has been the improvement of specification and standard quality. By grounding models in UML/SysML fragments and constrained natural language, and then subjecting them to model checking, animation, model-based testing, and abstract interpretation, the teams repeatedly exposed ambiguities, omissions, and inconsistencies that would otherwise have propagated to design and verification phases. In the 4SECURail experience, for example, the formalization of the RBC/RBC handover (from UNISIG artifacts) clarified subtle protocol corner cases and yielded actionable feedback for stakeholders. Similar effects were observed in ASTRail, where a structured comparison of tools against a moving-block design made explicit the trade-offs among analysis depth, usability, and integration potential. These results did not remain at the toy example level: even when the case studies were not product components, they were selected and parameterized to reflect realistic signaling scenarios so that the insights would transfer to practice.

Equally important has been the consolidation of repeatable engineering practices. Over time, the collaborations distilled safe modeling subsets, modeling guidelines for code generation, and practical back-to-back verification strategies that link models to code and test oracles. Combining techniques—model checking to reason about global safety and liveness, model-based testing to exercise behavior at scale and to drive regression, abstract interpretation to enforce runtime error freedom—proved more effective than relying on any single approach.

**Table 1.** Summary of Projects and Collaborations Involving Alessandro Fantechi

| Project | Topic | Outcome | Publications |
|---|---|---|---|
| Early Work | Formal Verification of Railway Systems | - Formal models of railway crossing and circular railway using CCS and ACTL.<br>- Verified safety and liveness properties with EMC and AMC model checkers.<br>- Validated fault-tolerance mechanisms for interlocking systems in the GUARDS project. | [46], [47], [6], [36], [35] |
| GE/Alstom Collaborations | Interlocking and ATP Systems, Requirements Analysis | - Validated SDL/Statechart models for interlockings with GE artifacts.<br>- Scalable model-extraction pipeline for fault finding and verification.<br>- Metrô Rio ATP case study with Simulink/Stateflow, reducing bugs and costs.<br>- 70% cost reduction in unit-level verification via model-based testing and abstract interpretation.<br>- NLP-based requirements defect detection with GATE/SREE tools. | [10], [9], [8], [11], [38], [37], [61], [62], [57], [58], [59], [72], [60], [66] |
| TRACE-IT | ATP, ATC, CBTC | - ATC demonstrator with deadlock-free CBTC strategy using UMC.<br>- Formal methods diversity study with 9 frameworks.<br>- CBTC global model with product line engineering and NLP-based requirements.<br>- Prototype tool for CBTC architecture. | [70], [69], [68], [65] |
| ASTRail | Formal Methods for Moving Block Signaling | - Comprehensive survey and evaluation of 14 FMs tools.<br>- Trial application of Simulink, UMC, and ProB to moving block systems.<br>- Increased industry awareness of FMs potential. | [7], [63], [56], [28], [64], [12], [15], [16] |
| 4SECURail | Formal Methods for RBC/RBC Handover Protocols | - FMs demonstrator identifying ambiguities in UNISIG standards.<br>- Publicly available UMC, ProB, and LNT models.<br>- Cost-benefit analysis showing economic advantages.<br>- Limited direct impact on standards due to absent infrastructure managers. | [1], [14], [2], [26], [25], [3], [33], [5], [32], [24] |
| STINGRAY | Smart Station Infrastructure (Energy Management) | - Prototypes for SCADA control of railroad switch heaters and EMS.<br>- Comparative analysis of SAN/Möbius and SHA/UPPAAL SMC.<br>- Generalized methodology for mapping automata to stochastic Petri nets.<br>- Spatial model checking future smart station lighting management. | [13], [18], [17], [19], [22], [21], [20], [23], [30] |
| MOST Spoke 4 | Predictive Maintenance, Digitization | - Data-driven real-time failure prediction for TCU using ARIMA, SARIMA, and ML (XGBoost), as well as by data-driven synthesis of stochastic fault tree models.<br>- User-centered dashboard design for Trenord's maintenance platform.<br>- Iterative requirements elicitation and AI-assisted prototyping. | [54], [42], [39] |

This methodological pluralism, backed by tool diversity and portable artefacts, reduced lock-in and created a robust basis for technology transfer and education.

The human capital dimension deserves explicit emphasis. The projects created concrete training pathways for students and early-career researchers, many of whom moved into industry or continued to collaborate on subsequent initiatives. This injection of *nuova linfa* into the CNR and partner organizations strengthened the European FM-for-rail community at large, building shared vocabularies, data sets, and habits of collaboration across academia, suppliers, and—when involved—standardization bodies. The pedagogical impact fed back into project execution: teams with mixed profiles (researchers, developers, assessors) were better able to negotiate the trade-offs between exploratory research and compliance-driven engineering.

### 8.2 Limitations

An honest appraisal of technology transfer also reveals structural frictions that cannot be glossed over. The most impactful studies are invariably those closest to real systems, yet working with real artefacts is constrained by confidentiality, the limited time windows typical of funded projects, and the academic and project pressure to produce publishable results early. These forces can limit scope, reduce reproducibility, and sometimes bias the selection of problems away from the most mission-critical ones. Integration with industrial development environments poses additional challenges: researchers and developers often operate with different stacks, expectations, and acceptance criteria, and the evidence required for certification demands stability, traceability, and process discipline that go beyond the lifecycle of a research prototype. Finally, the cost of industrial-grade verification frameworks—licensing, qualification, and toolchain customization—remains a significant barrier for academia and for many collaborative projects, constraining continuity, student training at scale, and open reproducibility.

Within this landscape, the project-specific contributions highlight both utility and limits. TRACE-IT delivered an ATS demonstrator and a formal deadlock analysis on a realistic CBTC-inspired layout, offering concrete strategies for avoiding system deadlocks and a proof-of-concept pipeline that can be adapted to similar metro contexts; confidentiality and the non-product status of the demonstrator, however, curtailed direct uptake into supplier processes. ASTRail produced a widely cited survey and a rigorous tool evaluation against moving-block requirements, giving decision-makers evidence-based guidance for selecting FM workflows; its academic case focus, by construction, limited deep embedding into OEM toolchains. 4SECURail showcased how formalization can strengthen standards, from early UML/SysML operational models through translations to multiple verification back ends, while coupling these steps to a cost-benefit analysis that articulated where FM activities return the most value; the absence of infrastructure managers as primary drivers, however, reduced the leverage on standardization timelines. STINGRAY, operating at station level, advanced the integration of SCADA and energy-management requirements and demonstrated how FM-informed design can clarify interfaces and operating constraints in heterogeneous environments; the diversity of station technologies slowed convergence on common tooling and limited generalization.

Beyond immediate artefacts and demonstrators, these collaborations opened new and durable lines of research. One such line concerns the semantics of practically useful, standards-friendly fragments of UML/SysML so that models can be verified without abandoning notations familiar to stakeholders. Another concerns end-to-end traceability from controlled natural language requirements to analyzable models and, ultimately, to test oracles and evidence packages suitable for CENELEC processes. A third line, motivated by the realities of industrial artefacts, investigates scalable model extraction and hybrid verification that combines static analysis, model checking, and runtime monitoring, while preserving arguments acceptable to assessors. Each of these lines has already yielded methods and tools that subsequent projects have reused and extended.

## 9 Conclusions and Outlook

This survey has retraced more than two decades of research and technology transfer on formal methods for railway systems carried out around the FMT laboratory at CNR–ISTI and in close collaboration with industrial partners, under the scientific leadership and vision of Alessandro Fantechi. Looking forward, the experiences surveyed here suggest a concrete and realistic outlook. The most sustainable path to impact begins with shared notations and controlled language, formalizes incrementally around high-risk behaviour, and engineers traceability and certification evidence from day one. Tool diversity should be embraced and orchestrated rather than minimized, with open artefacts and automation to keep pipelines maintainable as personnel and tools evolve. Crucially, budgets and planning must prioritize people as much as tools: effective transfer requires mixed teams with protected time for joint engineering, training, and maintenance of reproducible assets. On the ecosystem side, there is a clear need for affordable, open verification stacks, qualified subsets, and shared benchmarks that lower the activation energy for academia, SMEs, and standardization bodies. If these conditions are met, formal methods can continue to advance both as a scientific discipline and as a practical instrument for building and assuring the next generation of signaling and control systems.

There is increasing evidence for the successful application of formal methods in industry [29], not limited to the safety-critical domain including railways and other transportation sectors. The body of work reviewed in this paper confirms that formal methods can deliver concrete benefits—clearer standards and specifications, richer verification evidence, and better informed engineering decisions—provided that they are introduced with sensitivity to industrial realities and supported by the right mix of methods, tools, and people. The collaborations with GE Transportation, Alstom, and the broader consortium of European projects demonstrate that such a balance is achievable. The challenge, and the opportunity, is to scale these practices in a way that preserves scientific rigor while maximizing practical value for a sector where safety, reliability, and interoperability remain paramount.

**Acknowledgments.** The authors would like to thank Alessandro Fantechi for endless journeys involving formal methods and railways. After he left CNR in November 1992, he has always been associated with the CNR and also after he became professor at the University of Florence in 1995, he has continued to frequently take the train to Pisa to collaborate with the Formal Methods and Tools (FMT) lab, of which Alessandro has been a member from its foundation, more than two decades ago. The fact that FMT is internationally renowned for its expertise on the application of formal methods in the railway industry, is for a large part due to Alessandro.

The authors acknowledge the use of OpenAI ChatGPT and Grok for the revision of the phrasing and language of this manuscript.

Part of this work was carried out within the MUR PRIN 2022 PNRR P2022A492B project ADVENTURE (ADVancEd iNtegraTed evalUation of Railway systEms) and the MOST – Sustainable Mobility National Research Center and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4, COMPONENTE 2, INVESTIMENTO 1.4 – D.D. 1033 17/06/2022, CN00000023. This manuscript reflects only the authors' views and opinions, neither the European Union nor the European Commission can be considered responsible for them.

**Disclosure of Interests.** The authors have no competing interests to declare that are relevant to the content of this article.

## References

1. 4SECURail project Deliverable D2.1: Specification of formal development demonstrator (2020), https://projects.shift2rail.org/download.aspx?id=560cdd44-83e7-4f5d-879e-d8dcdf2e2b1b
2. 4SECURail project Deliverable D2.2: Formal development Demonstrator prototype, 1st Release (2020), https://projects.shift2rail.org/download.aspx?id=1761f4fa-c701-4321-b40c-3e67146ed482
3. 4SECURail project Deliverable D2.3: Case study requirements and specification (2020), https://projects.shift2rail.org/download.aspx?id=6917d0da-122f-41cb-8194-5f3e5029516b
4. 4SECURail project Deliverable D2.5: Formal development demonstrator prototype, final release" (2020), https://projects.shift2rail.org/download.aspx?id=eae0e50c-90fa-4408-b53c-f714e9dd2581
5. 4SECURail project Deliverable D2.6: Specification of cost/benefit analysis and learning curves, final release (2020), https://projects.shift2rail.org/download.aspx?id=ef729ed0-19d6-4378-aeb1-c74ced3edf50
6. Anselmi, A., Bernardeschi, C., Fantechi, A., Gnesi, S., Larosa, S., Mongardi, G., Torielli, F.: An Experience in Formal Verification of Safety Properties of a Railway Signalling Control System. In: Rabe, G. (ed.) Proceedings of the 14th International Conference on Computer Safety, Reliability and Security (SAFECOMP'95). pp. 474–488. Springer (1995). https://doi.org/10.1007/978-1-4471-3054-3_33
7. ASTRail project Deliverable D4.1: Report on Analysis and on Ranking of Formal Methods (2020), https://projects.shift2rail.org/download.aspx?id=dadd80d0-cf35-48d6-a1b7-b2a7545e37d6, accessed September 2025
8. Bacherini, S., Fantechi, A., Tempestini, M., Zingoni, N.: A Story About Formal Methods Adoption by a Railway Signaling Manufacturer. In: Misra, J., Nipkow, T.,

Sekerinski, E. (eds.) Proceedings of the 14th International Symposium on Formal Methods (FM'06). LNCS, vol. 4085, pp. 179–189. Springer (2006). https://doi.org/10.1007/11813040_13
9. Banci, M., Becucci, M., Fantechi, A., Spinicci, E.: Validation Coverage for a Component-based SDL Model of a Railway Signaling System. Electron. Notes Theor. Comput. **116**, 99–111 (2005). https://doi.org/10.1016/j.entcs.2004.02.083
10. Banci, M., Fantechi, A.: Geographical Versus Functional Modelling by Statecharts of Interlocking Systems. Electron. Notes Theor. Comput. **133**, 3–19 (2005). https://doi.org/10.1016/j.entcs.2004.08.055
11. Banci, M., Fantechi, A., Gnesi, S.: The Role of Formal Methods in Developing a Distributed Railway Interlocking System. In: Proceedings of the 5th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems (FORMS/FORMAT'04) (2004), https://iris.cnr.it/retrieve/32e02f77-2695-45de-9d94-cbea4e8a19ff/prod_120519-doc_125296.pdf
12. Basile, D., ter Beek, M.H., Ciancia, V.: Statistical Model Checking of a Moving Block Railway Signalling Scenario with Uppaal SMC: Experience and Outlook. In: Margaria, T., Steffen, B. (eds.) Proceedings of the 8th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation: Verification (ISoLA'18). LNCS, vol. 11245, pp. 372–391. Springer, Germany (2018). https://doi.org/10.1007/978-3-030-03421-4_24
13. Basile, D., ter Beek, M.H., Di Giandomenico, F., Fantechi, A., Gnesi, S., Spagnolo, G.O.: 30 Years of Simulation-Based Quantitative Analysis Tools: A Comparison Experiment Between Möbius and Uppaal SMC. In: Margaria, T., Steffen, B. (eds.) Proceedings of the 9th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation: Verification (ISoLA'20). LNCS, vol. 12476, pp. 368–384. Springer, Germany (2020). https://doi.org/10.1007/978-3-030-61362-4_21
14. Basile, D., ter Beek, M.H., Fantechi, A., Ferrari, A., Gnesi, S., Masullo, L., Mazzanti, F., Piattino, A., Trentini, D.: Designing a Demonstrator of Formal Methods for Railways Infrastructure Managers. In: Margaria, T., Steffen, B. (eds.) Proceedings of the 9th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation: Applications (ISoLA'20). LNCS, vol. 12478, pp. 467–485. Springer (2020). https://doi.org/10.1007/978-3-030-61467-6_30
15. Basile, D., ter Beek, M.H., Ferrari, A., Legay, A.: Modelling and Analysing ERTMS L3 Moving Block Railway Signalling with Simulink and Uppaal SMC. In: Larsen, K.G., Willemse, T. (eds.) Proceedings of the 24th International Conference on Formal Methods for Industrial Critical Systems (FMICS'19). LNCS, vol. 11687, pp. 1–21. Springer, Germany (2019). https://doi.org/10.1007/978-3-030-27008-7_1
16. Basile, D., ter Beek, M.H., Ferrari, A., Legay, A.: Exploring the ERTMS/ETCS full moving block specification: an experience with formal methods. Int. J. Softw. Tools Technol. Transf. **24**(3), 351–370 (2022). https://doi.org/10.1007/S10009-022-00653-3
17. Basile, D., Chiaradonna, S., Di Giandomenico, F., Gnesi, S.: A stochastic model-based approach to analyse reliable energy-saving rail road switch heating systems. J. Rail Transp. Plan. Manag. **6**(2), 163–181 (2016). https://doi.org/10.1016/j.jrtpm.2016.03.003
18. Basile, D., Chiaradonna, S., Di Giandomenico, F., Gnesi, S., Mazzanti, F.: Stochastic Model-Based Analysis of Energy Consumption in a Rail Road Switch Heating System. In: Fantechi, A., Pelliccione, P. (eds.) Proceedings of the 7th International Workshop on Software Engineering for Resilient Systems (SERENE'15). LNCS,

vol. 9274, pp. 82–98. Springer (2015). https://doi.org/10.1007/978-3-319-23129-7_7

19. Basile, D., Di Giandomenico, F., Gnesi, S.: Tuning Energy Consumption Strategies in the Railway Domain: A Model-Based Approach. In: Margaria, T., Steffen, B. (eds.) Proceedings of the 7th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications (ISoLA'16). LNCS, vol. 9953, pp. 315–330. Springer (2016). https://doi.org/10.1007/978-3-319-47169-3_23
20. Basile, D., Di Giandomenico, F., Gnesi, S.: A Refinement Approach to Analyse Critical Cyber-Physical Systems. In: Cerone, A., Roveri, M. (eds.) Revised Selected Papers of the SEFM 2017 Collocated Workshops: DataMod, FAACS, MSE, CoSim-CPS, and FOCLASA. LNCS, vol. 10729, pp. 267–283. Springer (2017). https://doi.org/10.1007/978-3-319-74781-1_19
21. Basile, D., Di Giandomenico, F., Gnesi, S.: Enhancing models correctness through formal verification: A case study from the railway domain. In: Pires, L.F., Hammoudi, S., Selic, B. (eds.) Proceedings of the 5th International Conference on Model-Driven Engineering and Software Development (MODELSWARD'17). pp. 679–686. SciTePress (2017). https://doi.org/10.5220/0006291106790686
22. Basile, D., Di Giandomenico, F., Gnesi, S.: Statistical Model Checking of an Energy-Saving Cyber-Physical System in the Railway Domain. In: Proceedings of the 32nd Symposium on Applied Computing (SAC'17). pp. 1356–1363. ACM (2017). https://doi.org/10.1145/3019612.3019824
23. Basile, D., Di Giandomenico, F., Gnesi, S.: On Quantitative Assessment of Reliability and Energy Consumption Indicators in Railway Systems. In: Kharchenko, V., Kondratenko, Y., Kacprzyk, J. (eds.) Green IT Engineering: Social, Business and Industrial Applications, Studies in Systems, Decision and Control, vol. 171, pp. 423–447. Springer (2018). https://doi.org/10.1007/978-3-030-00253-4_18
24. Basile, D., Fantechi, A., Rosadi, I.: Formal Analysis of the UNISIG Safety Application Intermediate Sub-layer: Applying Formal Methods to Railway Standard Interfaces. In: Lluch Lafuente, A., Mavridou, A. (eds.) Proceedings of the 26th International Conference on Formal Methods for Industrial Critical Systems (FMICS'21). LNCS, vol. 12863, pp. 174–190. Springer (2021). https://doi.org/10.1007/978-3-030-85248-1_11
25. Basile, D., Mazzanti, F.: Comparing Model Checking and Model-based Simulation. In: ter Beek, M.H., Collart-Dutilleul, S., Lecomte, T. (eds.) Proceedings of the 6th International Conference on Reliability, Safety, and Security of Railway Systems: Modelling, Analysis, Verification, and Certification (RSSRail'25). LNCS, vol. 16236, pp. 135–155. Springer (2025). https://doi.org/10.1007/978-3-032-10762-6_12
26. Basile, D., Mazzanti, F., Ferrari, A.: Experimenting with Formal Verification and Model-Based Development in Railways: The Case of UMC and Sparx Enterprise Architect. In: Cimatti, A., Titolo, L. (eds.) Proceedings of the 28th International Conference on Formal Methods for Industrial Critical Systems (FMICS'23). LNCS, vol. 14290, pp. 1–21. Springer (2023). https://doi.org/10.1007/978-3-031-43681-9_1
27. ter Beek, M.H.: Models for formal methods and tools: the case of railway systems. Softw. Syst. Model. **24**(6) (2025). https://doi.org/10.1007/s10270-025-01276-3
28. ter Beek, M.H., Borälv, A., Fantechi, A., Ferrari, A., Gnesi, S., Löfving, C., Mazzanti, F.: Adopting Formal Methods in an Industrial Setting: The Railways Case. In: ter Beek, M.H., McIver, A., Oliveira, J.N. (eds.) Proceedings of the 3rd World

Congress on Formal Methods: The Next 30 Years (FM'19). LNCS, vol. 11800, pp. 762–772. Springer (2019). https://doi.org/10.1007/978-3-030-30942-8_46
29. ter Beek, M.H., Chapman, R., Cleaveland, R., Garavel, H., Gu, R., ter Horst, I., Keiren, J.J.A., Lecomte, T., Leuschel, M., Rozier, K.Y., Sampaio, A., Seceleanu, C., Thomas, M., Willemse, T.A.C., Zhang, L.: Formal Methods in Industry. Formal Aspects Comput. **37**(1), 7:1–7:38 (2025). https://doi.org/10.1145/3689374
30. ter Beek, M.H., Ciancia, V., Latella, D., Massink, M., Spagnolo, G.O.: Spatial Model Checking for Smart Stations: Research Challenges. In: Lluch Lafuente, A., Mavridou, A. (eds.) Proceedings of the 26th International Conference on Formal Methods for Industrial Critical Systems (FMICS'21). LNCS, vol. 12863, pp. 39–47. Springer, Germany (2021). https://doi.org/10.1007/978-3-030-85248-1_3
31. ter Beek, M.H., Fantechi, A., Gnesi, S.: Formal Methods for Industrial Critical Systems: 30 Years of Railway Applications. In: Hinchey, M., Steffen, B. (eds.) The Combined Power of Research, Education, and Dissemination. LNCS, vol. 15240, pp. 327–344. Springer (2025). https://doi.org/10.1007/978-3-031-73887-6_21
32. Belli, D., Fantechi, A., Gnesi, S., Masullo, L., Mazzanti, F., Quadrini, L., Trentini, D., Vaghi, C.: The 4SECURail Case Study on Rigorous Standard Interface Specifications. In: Cimatti, A., Titolo, L. (eds.) Proceedings of the 28th International Conference on Formal Methods for Industrial Critical Systems (FMICS'23). LNCS, vol. 14290, pp. 22–39. Springer (2023). https://doi.org/10.1007/978-3-031-43681-9_2
33. Belli, D., Mazzanti, F.: A Case Study in Formal Analysis of System Requirements. In: Masci, P., Bernardeschi, C., Graziani, P., Koddenbrock, M., Palmieri, M. (eds.) Revised Selected Papers of the SEFM 2022 Collocated Workshops: AI4EA, F-IDE, CoSim-CPS, CIFMA. LNCS, vol. 13765, pp. 164–173. Springer (2022). https://doi.org/10.1007/978-3-031-26236-4_14
34. Belmonte, G., Ciancia, V., Latella, D., Massink, M.: VoxLogicA: A Spatial Model Checker for Declarative Image Analysis. In: Vojnar, T., Zhang, L. (eds.) Proceedings of the 25th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'19). LNCS, vol. 11427, pp. 281–298. Springer, Germany (2019). https://doi.org/10.1007/978-3-030-17462-0_16
35. Bernardeschi, C., Fantechi, A., Gnesi, S.: Formal validation of fault-tolerance mechanisms inside GUARDS. Reliab. Eng. Syst. Safety **71**(3), 261–270 (2001). https://doi.org/10.1016/S0951-8320(00)00078-8
36. Bernardeschi, C., Fantechi, A., Gnesi, S., Larosa, S., Mongardi, G., Romano, D.: A Formal Verification Environment for Railway Signaling System Design. Formal Methods Syst. Des. **12**(2), 139–161 (1998). https://doi.org/10.1023/A:1008645826258
37. Bonacchi, A., Fantechi, A.: Validation of Interlocking Systems by Testing their Models. In: Proceedings of the 9th International Conference on the Quality of Information and Communications Technology (QUATIC'14). pp. 226–229. IEEE (2014). https://doi.org/10.1109/QUATIC.2014.37
38. Bonacchi, A., Fantechi, A., Bacherini, S., Tempestini, M.: Validation Process for Railway Interlocking Systems. Sci. Comput. Program. **128**, 2–21 (2016). https://doi.org/10.1016/j.scico.2016.04.004
39. Broccia, G., Borselli, A., Cefaloni, M.R., Delcorno, F., Ferrari, A.: An Experience Report on Leveraging LLMs for GUI Generation: Automating Coding to Prioritise Creativity. In: Proceedings of the 12th International Workshop on Creativity in Requirements Engineering (CreaRE'25) co-located with the 31st International Conference on Requirements Engineering: Foundation for Software Quality (REFSQ'25). CEUR Workshop Proceedings, vol. 3964 (2025), https://ceur-ws.org/Vol-3959/CreaRE-paper2.pdf

40. Broy, M., Brucker, A.D., Fantechi, A., Gleirscher, M., Havelund, K., Kuppe, M.A., Mendes, A., Platzer, A., Ringert, J.O., Sullivan, A.: Does Every Computer Scientist Need to Know Formal Methods? Formal Aspects Comput. **37**(1), 6:1–6:17 (2025). https://doi.org/10.1145/3670795
41. Broy, M., Cengarle, M.V.: UML formal semantics: lessons learned. Softw. Syst. Model. **10**(4), 441–446 (2011). https://doi.org/10.1007/s10270-011-0207-y
42. Carnevali, L., Fantechi, A., Gori, G., Vreshtazi, D., Borselli, A., Cefaloni, M.R., Rota, L.: Data-Driven Synthesis of Stochastic Fault Trees for Proactive Maintenance of Railway Vehicles. In: Remke, A., Steffen, B. (eds.) Proceedings of the 30th International Conference on Formal Methods for Industrial Critical Systems (FMICS'25). LNCS, vol. 16040, pp. 162–181. Springer (2025). https://doi.org/10.1007/978-3-032-00942-5_9
43. Clarke, E.M., Emerson, E.A., Sistla, A.P.: Automatic Verification of Finite State Concurrent Systems Using Temporal Logic Specifications: A Practical Approach. In: Conference Record of the 10th Annual ACM Symposium on Principles of Programming Languages (POPL'83). pp. 117–126. ACM (1983). https://doi.org/10.1145/567067.567080
44. Clarke, E.M., Emerson, E.A., Sistla, A.P.: Automatic Verification of Finite-State Concurrent Systems Using Temporal Logic Specifications. ACM Trans. Program. Lang. Syst. **8**(2), 244–263 (1986). https://doi.org/10.1145/5397.5399
45. Cook, S.: Looking back at UML. Softw. Syst. Model. **11**(4), 471–480 (2012). https://doi.org/10.1007/s10270-012-0256-x
46. De Nicola, R., Fantechi, A., Gnesi, S., Ristori, G.: An Action Based Framework for Verifying Logical and Behavioural Properties of Concurrent Systems. In: Larsen, K.G., Skou, A. (eds.) Proceedings of the 3rd International Workshop on Computer Aided Verification (CAV'91). LNCS, vol. 575, pp. 37–47. Springer (1991). https://doi.org/10.1007/3-540-55179-4_5
47. De Nicola, R., Fantechi, A., Gnesi, S., Ristori, G.: An Action-Based Framework for Verifying Logical and Behavioural Properties of Concurrent Systems. Comput. Networks ISDN Syst. **25**(7), 761–778 (1993). https://doi.org/10.1016/0169-7552(93)90047-8
48. De Nicola, R., Vaandrager, F.W.: Three Logics for Branching Bisimulation: Extended Abstract. In: Proceedings of the 4th Annual Symposium on Logic in Computer Science (LICS'89). pp. 118–129. IEEE (1990). https://doi.org/10.1109/LICS.1990.113739
49. De Nicola, R., Vaandrager, F.W.: Three Logics for Branching Bisimulation. J. ACM **42**(2), 458–487 (1995). https://doi.org/10.1145/201019.201032
50. Derezińska, A., Szczykulski, M.: Interpretation Problems in Code Generation from UML State Machines: a Comparative Study. In: Kwater, T., Zuberek, W.M., Ciarkowski, A., Kruk, M., Pekala, R., Twaróg, B. (eds.) Proceedings of the 2nd Scientific Conference on Computing in Science and Technology (CSI'11). pp. 36–50. Monographs in Applied Informatics, Warsaw University of Life Sciences (2012), https://repo.pw.edu.pl/docstore/download/WEiTI-1e8d2c48-b87c-476f-94d6-cc9df9319050/ADerSzczy.pdf
51. Fantechi, A.: The Role of Formal Methods in Software Development for Railway Applications. In: Flammini, F. (ed.) Railway Safety, Reliability, and Security: Technologies and Systems Engineering, chap. 12, pp. 282–297. IGI Global (2012). https://doi.org/10.4018/978-1-4666-1643-1.ch012
52. Fantechi, A.: Twenty-Five Years of Formal Methods and Railways: What Next? In: Counsell, S., Núñez, M. (eds.) Revised Selected Papers of the SEFM 2013

Collocated Workshops: BEAT2, WS-FMDS, FM-RAIL-Bok, MoKMaSD, and OpenCert. LNCS, vol. 8368, pp. 167–183. Springer (2013). https://doi.org/10.1007/978-3-319-05032-4_13

53. Fantechi, A., Fokkink, W., Morzenti, A.: Some Trends in Formal Methods Applications to Railway Signaling. In: Gnesi, S., Margaria, T. (eds.) Formal Methods for Industrial Critical Systems: A Survey of Applications, chap. 4, pp. 61–84. Wiley (2013). https://doi.org/10.1002/9781118459898.ch4
54. Ferdous, R., Spagnolo, G., Borselli, A., Rota, L., Ferrari, A.: Identifying maintenance needs with machine learning: a case study in railways. In: Proceedings of the 11th International Workshop on Artificial Intelligence and Requirements Engineering (AIRE'24) of the 32nd International Requirements Engineering Conference (RE'24). pp. 22–25. IEEE (2024). https://doi.org/10.1109/REW61692.2024.00008
55. Ferrari, A., ter Beek, M.H.: Formal Methods in Railways: a Systematic Mapping Study. ACM Comput. Surv. **55**(4), 69:1–69:37 (2023). https://doi.org/10.1145/3520480
56. Ferrari, A., ter Beek, M.H., Mazzanti, F., Basile, D., Fantechi, A., Gnesi, S., Piattino, A., Trentini, D.: Survey on Formal Methods and Tools in Railways: The ASTRail Approach. In: Collart-Dutilleul, S., Lecomte, T., Romanovsky, A. (eds.) Proceedings of the 3rd International Conference on Reliability, Safety, and Security of Railway Systems: Modelling, Analysis, Verification, and Certification (RSSRail'19). LNCS, vol. 11495, pp. 226–241. Springer (2019). https://doi.org/10.1007/978-3-030-18744-6_15
57. Ferrari, A., Fantechi, A., Bacherini, S., Zingoni, N.: Modeling Guidelines for Code Generation in the Railway Signaling Context. In: Proceedings of the 1st NASA Formal Methods Symposium (NFM'09). pp. 166–170. NASA Technical Reports Server, NASA (2009), https://ntrs.nasa.gov/api/citations/20100024476/downloads/20100024476.pdf
58. Ferrari, A., Fantechi, A., Gnesi, S.: Lessons Learnt from the Adoption of Formal Model-Based Development. In: Goodloe, A., Person, S. (eds.) Proceedings of the 4th International Symposium NASA Formal Methods (NFM'12). LNCS, vol. 7226, pp. 24–38. Springer (2012). https://doi.org/10.1007/978-3-642-28891-3_5
59. Ferrari, A., Fantechi, A., Gnesi, S., Magnani, G.: Model-Based Development and Formal Methods in the Railway Industry. IEEE Softw. **30**(3), 28–34 (2013). https://doi.org/10.1109/MS.2013.44
60. Ferrari, A., Gori, G., Rosadini, B., Trotta, I., Bacherini, S., Fantechi, A., Gnesi, S.: Detecting requirements defects with NLP patterns: an industrial experience in the railway domain. Empir. Softw. Eng. **23**, 3684–3733 (2018). https://doi.org/10.1007/s10664-018-9596-7
61. Ferrari, A., Grasso, D., Magnani, G., Fantechi, A., Tempestini, M.: The Metrô Rio Case Study. Sci. Comput. Program. **78**(8), 951–970 (2013). https://doi.org/10.1016/j.scico.2012.04.003
62. Ferrari, A., Magnani, G., Grasso, D., Fantechi, A., Tempestini, M.: Adoption of Model-Based Testing and Abstract Interpretation by a Railway Signalling Manufacturer. Int. J. Embed. Real-Time Commun. Syst. **2**(2), 42–61 (2011). https://doi.org/10.4018/jertcs.2011040103
63. Ferrari, A., Mazzanti, F., Basile, D., ter Beek, M.H.: Systematic Evaluation and Usability Analysis of Formal Methods Tools for Railway Signaling System Design. IEEE Trans. Softw. Eng. **48**(11), 4675–4691 (2022). https://doi.org/10.1109/TSE.2021.3124677

64. Ferrari, A., Mazzanti, F., Basile, D., ter Beek, M.H., Fantechi, A.: Comparing Formal Tools for System Design: a Judgment Study. In: Proceedings of the 42nd International Conference on Software Engineering (ICSE'20). pp. 62–74. ACM (2020). https://doi.org/10.1145/3377811.3380373
65. Ferrari, A., Spagnolo, G.O., Martelli, G., Menabeni, S.: From commercial documents to system requirements: an approach for the engineering of novel CBTC solutions. Int. J. Softw. Tools Technol. Transf. **16**(6), 647–667 (2014). https://doi.org/10.1007/s10009-013-0298-6
66. Ferrari, A., Spoletini, P.: Formal requirements engineering and large language models: A two-way roadmap. Inf. Softw. Technol. **181**, 107697 (2025). https://doi.org/10.1016/j.infsof.2025.107697
67. Mazzanti, F., Belli, D.: The 4SECURail Formal Methods Demonstrator. In: Collart-Dutilleul, S., Haxthausen, A.E., Lecomte, T. (eds.) Proceedings of the 4th International Conference on Reliability, Safety, and Security of Railway Systems: Modelling, Analysis, Verification, and Certification (RSSRail'22). LNCS, vol. 13294, pp. 149–165. Springer (2022). https://doi.org/10.1007/978-3-031-05814-1_11
68. Mazzanti, F., Ferrari, A.: Ten Diverse Formal Models for a CBTC Automatic Train Supervision System. In: Gallagher, J.P., van Glabbeek, R., Serwe, W. (eds.) Proceedings of the 3rd Workshop on Models for Formal Analysis of Real Systems and the 6th International Workshop on Verification and Program Transformation (MARS/VPT'18). EPTCS, vol. 268, pp. 104–149 (2018). https://doi.org/10.4204/EPTCS.268.4
69. Mazzanti, F., Ferrari, A., Spagnolo, G.O.: Towards formal methods diversity in railways: an experience report with seven frameworks. Int. J. Softw. Tools Technol. Transf. **20**(3), 263–288 (2018). https://doi.org/10.1007/s10009-018-0488-3
70. Mazzanti, F., Ferrari, A., Spagnolo, G.O.: Experiments in Formal Modelling of a Deadlock Avoidance Algorithm for a CBTC System. In: Margaria, T., Steffen, B. (eds.) Proceedings of the 7th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications (ISoLA'16). LNCS, vol. 9953, pp. 297–314 (2016). https://doi.org/10.1007/978-3-319-47169-3_22
71. Mazzanti, F., Spagnolo, G.O., Della Longa, S., Ferrari, A.: Deadlock Avoidance in Train Scheduling: A Model Checking Approach. In: Lang, F., Flammini, F. (eds.) Proceedings of the 19th International Conference on Formal Methods for Industrial Critical Systems (FMICS'14). LNCS, vol. 8718, pp. 109–123. Springer (2014). https://doi.org/10.1007/978-3-319-10702-8_8
72. Rosadini, B., Ferrari, A., Gori, G., Fantechi, A., Gnesi, S., Trotta, I., Bacherini, S.: Using NLP to detect requirements defects: An industrial experience in the railway domain. In: Grünbacher, P., Perini, A. (eds.) Proceedings of the 23rd International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ'17). LNCS, vol. 10153, pp. 344–360. Springer (2017). https://doi.org/10.1007/978-3-319-54045-0_24
73. Shift2Rail: 4SECURail project site, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=s2r_4securail, accessed September 2025
74. Shift2Rail: ASTRail project site, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=S2R_ASTRAIL, accessed September 2025